Lab 2

Since seedlabs said from vm or attacker, i ran from vm since i was using python environments that caused issues with permissions

Q1 Packet Sniffing and Spoofing

1.1

```
## List Network Interfaces
from scapy.all import get_if_list
print(get_if_list())
```

```
def print_pkt(pkt):
    pkt.show()
pkt = sniff(iface="br-407b98f0a521", filter="icmp", prn=print_pkt)
```

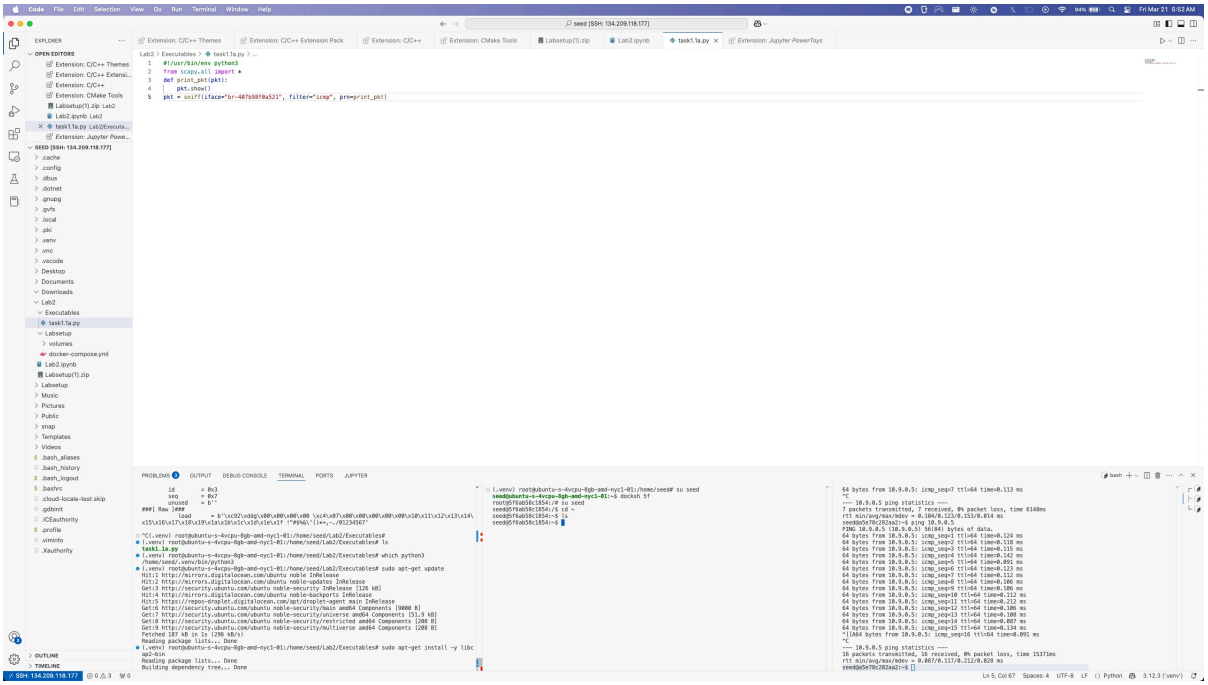
1.2

ICMP

1.3

"ping" command uses the Internet Control Message Protocol (ICMP) to test network connectivity:

we ping seed@5f6ab58c1854 from seed@a5e78c282aa2



1.4

Capture any TCP packet that comes from a specific IP and with a destination port number 23.

Your code must include the following: (1) capture TCP; (2) capture from any specific IP address; and (3) capture to destination port 23.

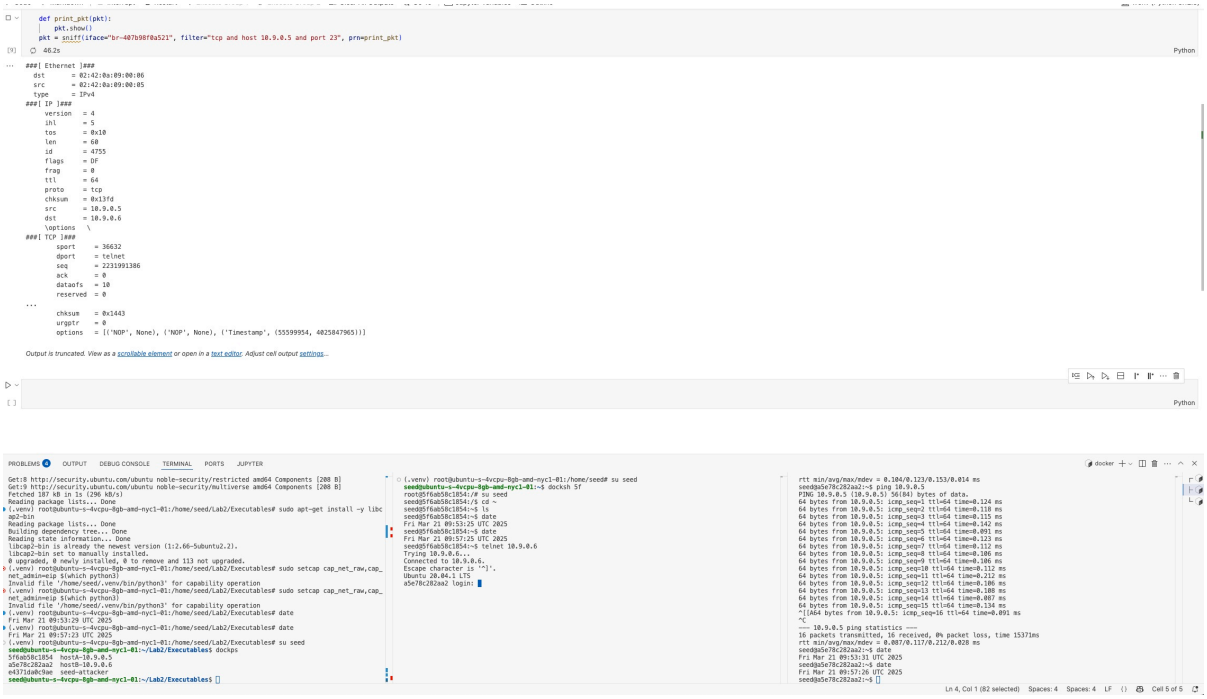
Hint: Use the attacker machine and write your code for sniffing. Then generate telnet traffic from the attacker machine to test that your program works.

tcp and host 10.9.0.1 and port 23

1.5

```
def print_pkt(pkt):
    pkt.show()
pkt = sniff(iface="br-407b98f0a521", filter="tcp and host 10.9.0.5 and port
23", prn=print_pkt)
```

Used one of the machines for simplicity:



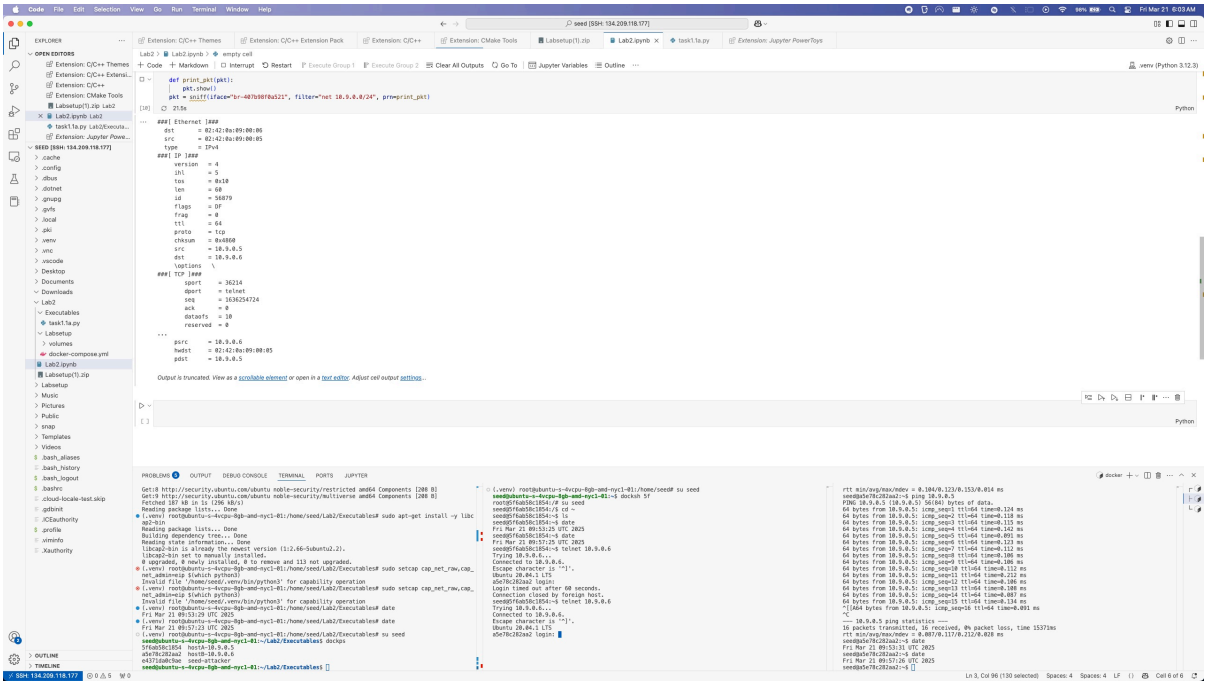
1.6

net 10.9.0.0/24

1.7

```
def print_pkt(pkt):
    pkt.show()
pkt = sniff(iface="br-407b98f0a521", filter="net 10.9.0.0/24",
prn=print_pkt)
```

Used one of the machines for simplicity:



Q2 Spoofing ICMP Packets

2.1

Spoof an ICMP echo request packet with source IP address 8.8.8.8 and send to Host A. Use Wireshark to show that it replies back with echo replies.

```
from scapy.all import *
packet = IP(src="8.8.8.8", dst="10.9.0.5") / ICMP()
send(packet)
```

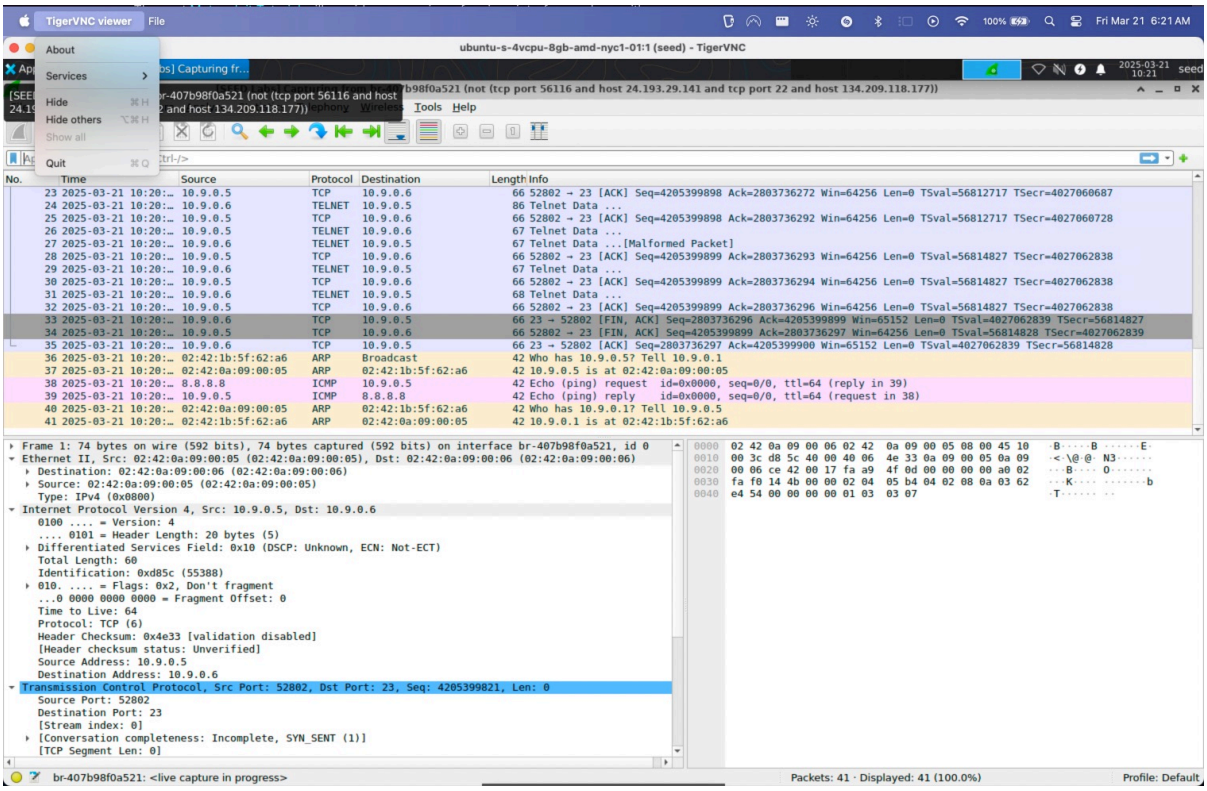
Based on the code above, what is the IP address for (1)?

8.8.8.8

Based on the code above, what is the IP address for (2)?

10.9.0.5

2.2



Q3 Fully-automated Traceroute

Using the skeleton code below, implement ICMP traceroute using scapy. Do NOT use the built-in scapy traceroute function. Perform a traceroute to 8.8.8.8. Show proof using a Wireshark capture and take a screenshot of your program's output.

3.1

- A: 1
- B: 8.8.8.8
- C: packet[ICMP].type

Q4 Sniffing and then spoofing program

Ubuntu traceroute gives:

```
TTL: 10, Source:  8.8.8.8
root@ubuntu-s-4vcpu-8gb-amd-nyc1-01:/home/seed/Lab2/Executables# traceroute -I 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  * * *
 2  10.71.5.154 (10.71.5.154)  1.680 ms  1.673 ms  1.667 ms
 3  * * *
 4  143.244.192.156 (143.244.192.156)  1.538 ms  1.532 ms  1.526 ms
 5  143.244.225.84 (143.244.225.84)  1.966 ms  1.960 ms  2.021 ms
 6  143.244.225.19 (143.244.225.19)  1.841 ms  0.787 ms  0.733 ms
 7  146.190.180.27 (146.190.180.27)  2.594 ms  2.617 ms  2.600 ms
 8  142.251.249.123 (142.251.249.123)  3.197 ms  3.097 ms  3.005 ms
 9  142.250.224.247 (142.250.224.247)  2.597 ms  2.567 ms  2.147 ms
10  dns.google (8.8.8.8)  1.418 ms  1.131 ms  1.112 ms
root@ubuntu-s-4vcpu-8gb-amd-nyc1-01:/home/seed/Lab2/Executables#
```

or

```
root@ubuntu-s-4vcpu-8gb-amd-nyc1-01:/home/seed/Lab2/Executables# traceroute -I 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  * * *
 2  10.71.5.156 (10.71.5.156)  1.581 ms  1.574 ms  1.568 ms
 3  138.197.248.76 (138.197.248.76)  2.012 ms * *
 4  143.244.192.152 (143.244.192.152)  1.182 ms  1.177 ms  1.171 ms
 5  143.244.225.84 (143.244.225.84)  2.024 ms  2.018 ms  2.013 ms
 6  143.244.225.19 (143.244.225.19)  1.402 ms  0.772 ms  0.729 ms
 7  146.190.180.27 (146.190.180.27)  2.662 ms  2.418 ms  2.285 ms
 8  142.251.249.123 (142.251.249.123)  1.612 ms  1.597 ms  1.328 ms
 9  142.250.224.247 (142.250.224.247)  2.442 ms  2.497 ms  2.485 ms
10  dns.google (8.8.8.8)  1.481 ms  1.426 ms  1.143 ms
```

depending on how it feels...

So many attempts:

v1

```python
#!/usr/bin/env python3
from scapy.all import IP, ICMP, sr1

ttl=1
destination="8.8.8.8"

while True:
    ip = IP(dst="8.8.8.8", ttl=ttl)

    icmp = ICMP()

    packet = sr1(ip / icmp, verbose=0)

    if packet[ICMP].type == 0:
        print("Complete ", packet[IP].src)
        break
    else:
        print("TTL: %d, Source: " %ttl, packet[IP].src)
        ttl+= 1
```

v2

```python
# Hangs at 5
#!/usr/bin/env python3
from scapy.all import IP, ICMP, sr1

ttl=6
destination="8.8.8.8"

while True:
    ip = IP(dst="8.8.8.8", ttl=ttl)
```

```
    icmp = ICMP()

    packet = sr1(ip / icmp, verbose=0)

    if packet[ICMP].type == 0:
        print("Complete ", packet[IP].src)
        break
    else:
        print("TTL: %d, Source: " %ttl, packet[IP].src)
        ttl+= 1
```

v3

```
#!/usr/bin/env python3
from scapy.all import IP, ICMP, sr1

ttl=1
destination="8.8.8.8"

while True:
    ip = IP(dst="8.8.8.8", ttl=ttl)

    icmp = ICMP()

    packet = sr1(ip / icmp, timeout=2,verbose=0)

    if packet is None:
        print(f"TTL {ttl}: No response")
        ttl += 1
        continue

    if packet[ICMP].type == 0:
        print("Complete ", packet[IP].src)
        break
    else:
        print("TTL: %d, Source: " %ttl, packet[IP].src)
        ttl+= 1
```

v4

```
#!/usr/bin/env python3
from scapy.all import IP, ICMP, sr1

ttl=1
destination="8.8.8.8"
```

```
while True:
    ip = IP(dst="8.8.8.8", ttl=ttl)

    icmp = ICMP()

    packet = sr1(ip / icmp, timeout=3, retry=3, verbose=0)

    if packet is None:
        print(f"TTL {ttl}: No response")
        ttl += 1
        continue

    if packet[ICMP].type == 0:
        print("Complete ", packet[IP].src)
        break
    else:
        print("TTL: %d, Source: " %ttl, packet[IP].src)
        ttl+= 1
```

v5

```
#!/usr/bin/env python3
from scapy.all import IP, ICMP, sr1, Raw

ttl=1
destination="8.8.8.8"

while True:
    ip = IP(dst="8.8.8.8", ttl=ttl)

    icmp = ICMP()

    packet = IP(dst="8.8.8.8", ttl=5) / ICMP() / Raw(load="HelloRouter")

    packet = sr1(packet, timeout=3, retry=3, verbose=0)

    if packet is None:
        print(f"TTL {ttl}: No response")
        ttl += 1
        continue

    if packet[ICMP].type == 0:
        print("Complete ", packet[IP].src)
        break
    else:
        print("TTL: %d, Source: " %ttl, packet[IP].src)
        ttl+= 1
```

V4 Out:

```
#!/usr/bin/env python3
from scapy.all import IP, ICMP, sr1

ttl=1
destination="8.8.8.8"

while True:
    ip = IP(dst="8.8.8.8", ttl=ttl)

    icmp = ICMP()

    packet = sr1(ip / icmp, timeout=3, retry=3, verbose=0)

    if packet is None:
        print(f"TTL {ttl}: No response")
        ttl += 1
        continue

    if packet[ICMP].type == 0:
        print("Complete ", packet[IP].src)
        break
    else:
        print("TTL: %d, Source: " %ttl, packet[IP].src)
        ttl+= 1
```

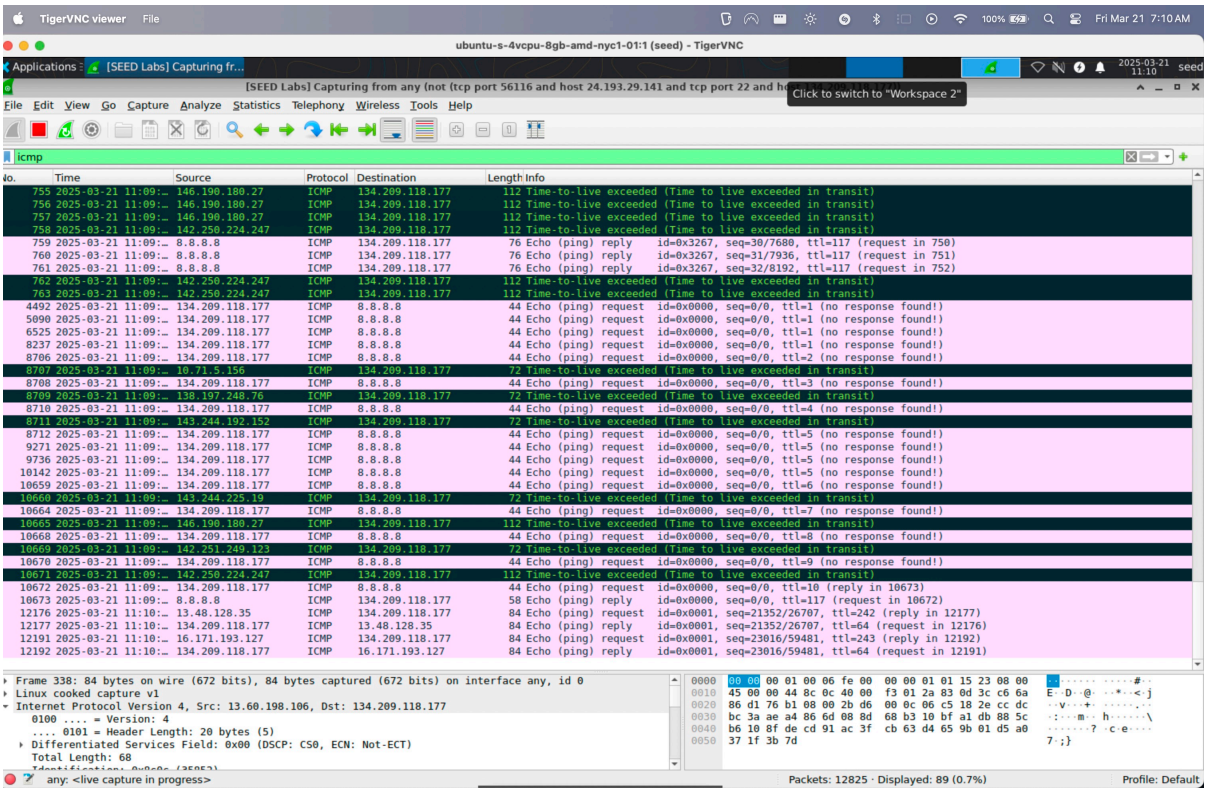
✓ 24.3s

```
TTL 1: No response
TTL: 2, Source:  10.71.5.156
TTL: 3, Source:  138.197.248.76
TTL: 4, Source:  143.244.192.152
TTL 5: No response
TTL: 6, Source:  143.244.225.19
TTL: 7, Source:  146.190.180.27
TTL: 8, Source:  142.251.249.123
TTL: 9, Source:  142.250.224.247
Complete  8.8.8.8
```

Final Version:

```
#!/usr/bin/env python3
from scapy.all import IP, ICMP, sr1

ttl=1
destination="8.8.8.8"

while True:
    ip = IP(dst="8.8.8.8", ttl=ttl)

    icmp = ICMP()
```

```
    packet = sr1(ip / icmp, timeout=3, retry=2, verbose=0)

    if packet is None:
        print(f"TTL {ttl}: No response")
        ttl += 1
        continue
    elif ttl >= 11:
        break
    elif packet.type == 3:
        print("Complete ", packet[IP].src)
        break
    else:
        print("TTL: %d, Source: " %ttl, packet[IP].src)
        ttl+= 1
```


TigerVNC viewer File
Fri Mar 21 7:10 AM
ubuntu-s-4vcpu-8gb-amd-nyc1-01:1 (seed) - TigerVNC
Applications [SEED Labs] Capturing fr...
2025-03-21 11:10 seed
[SEED Labs] Capturing from any (not (tcp port 56116 and host 24.193.29.141 and tcp port 22 and ho
Click to switch to "Workspace 2"
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Time Source Protocol Destination Length Info
755 2025-03-21 11:09:... 146.190.180.27 ICMP 134.209.118.177 112 Time-to-live exceeded (Time to live exceeded in transit)
756 2025-03-21 11:09:... 146.190.180.27 ICMP 134.209.118.177 112 Time-to-live exceeded (Time to live exceeded in transit)
757 2025-03-21 11:09:... 146.190.180.27 ICMP 134.209.118.177 112 Time-to-live exceeded (Time to live exceeded in transit)
758 2025-03-21 11:09:... 142.250.224.247 ICMP 134.209.118.177 112 Time-to-live exceeded (Time to live exceeded in transit)
759 2025-03-21 11:09:... 8.8.8.8 ICMP 134.209.118.177 76 Echo (ping) reply id=0x3267, seq=30/7680, ttl=117 (request in 750)
760 2025-03-21 11:09:... 8.8.8.8 ICMP 134.209.118.177 76 Echo (ping) reply id=0x3267, seq=31/7936, ttl=117 (request in 751)
761 2025-03-21 11:09:... 8.8.8.8 ICMP 134.209.118.177 76 Echo (ping) reply id=0x3267, seq=32/8192, ttl=117 (request in 752)
762 2025-03-21 11:09:... 142.250.224.247 ICMP 134.209.118.177 112 Time-to-live exceeded (Time to live exceeded in transit)
763 2025-03-21 11:09:... 142.250.224.247 ICMP 134.209.118.177 112 Time-to-live exceeded (Time to live exceeded in transit)
4492 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=1 (no response found!)
5090 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=1 (no response found!)
6525 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=1 (no response found!)
8237 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=1 (no response found!)
8706 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=2 (no response found!)
8707 2025-03-21 11:09:... 10.71.5.156 ICMP 134.209.118.177 72 Time-to-live exceeded (Time to live exceeded in transit)
8708 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=3 (no response found!)
8709 2025-03-21 11:09:... 138.197.248.76 ICMP 134.209.118.177 72 Time-to-live exceeded (Time to live exceeded in transit)
8710 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=4 (no response found!)
8711 2025-03-21 11:09:... 143.244.192.152 ICMP 134.209.118.177 72 Time-to-live exceeded (Time to live exceeded in transit)
8712 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=5 (no response found!)
9271 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=5 (no response found!)
9736 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=5 (no response found!)
10142 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=5 (no response found!)
10659 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=6 (no response found!)
10660 2025-03-21 11:09:... 143.244.225.19 ICMP 134.209.118.177 72 Time-to-live exceeded (Time to live exceeded in transit)
10664 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=7 (no response found!)
10665 2025-03-21 11:09:... 146.190.180.27 ICMP 134.209.118.177 112 Time-to-live exceeded (Time to live exceeded in transit)
10668 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=8 (no response found!)
10669 2025-03-21 11:09:... 142.251.249.123 ICMP 134.209.118.177 72 Time-to-live exceeded (Time to live exceeded in transit)
10670 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=9 (no response found!)
10671 2025-03-21 11:09:... 142.250.224.247 ICMP 134.209.118.177 112 Time-to-live exceeded (Time to live exceeded in transit)
10672 2025-03-21 11:09:... 134.209.118.177 ICMP 8.8.8.8 44 Echo (ping) request id=0x0000, seq=0/0, ttl=10 (reply in 10673)
10673 2025-03-21 11:09:... 8.8.8.8 ICMP 134.209.118.177 58 Echo (ping) reply id=0x0000, seq=0/0, ttl=117 (request in 10672)
12176 2025-03-21 11:10:... 13.48.128.35 ICMP 134.209.118.177 84 Echo (ping) request id=0x0001, seq=21352/26707, ttl=242 (reply in 12177)
12177 2025-03-21 11:10:... 134.209.118.177 ICMP 13.48.128.35 84 Echo (ping) reply id=0x0001, seq=21352/26707, ttl=64 (request in 12176)
12191 2025-03-21 11:10:... 16.171.193.127 ICMP 134.209.118.177 84 Echo (ping) request id=0x0001, seq=23016/59481, ttl=243 (reply in 12192)
12192 2025-03-21 11:10:... 134.209.118.177 ICMP 16.171.193.127 84 Echo (ping) reply id=0x0001, seq=23016/59481, ttl=64 (request in 12191)
Frame 338: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 13.60.198.106, Dst: 134.209.118.177
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 68
0000 00 00 00 01 00 06 fe 00 00 00 01 01 15 23 08 00
0010 45 00 00 44 8c 0c 40 00 f3 01 2a 83 0d 3c c6 6a
0020 86 d1 76 b1 08 00 2b d6 00 0c 06 c5 18 2e cc dc
0030 bc 3a ae a4 86 6d 08 8d 68 b3 10 bf a1 db 88 5c
0040 b6 10 8f de cd 91 ac 3f cb 63 d4 65 9b 01 d5 a0
0050 37 1f 3b 7d
any: <live capture in progress>
Packets: 12825 · Displayed: 89 (0.7%)
Profile: Default

Lab2 > Executables > traceroute.py > ...

```python
#!/usr/bin/env python3
from scapy.all import IP, ICMP, sr1

ttl=1
destination="8.8.8.8"

while True:
    ip = IP(dst="8.8.8.8", ttl=ttl)

    icmp = ICMP()

    packet = sr1(ip / icmp, timeout=3, retry=2, verbose=0)

    if packet is None:
        print(f"TTL {ttl}: No response")
        ttl += 1
        continue
    elif ttl >= 11:
        break
    elif packet.type == 3:
        print("Complete ", packet[IP].src)
        break
    else:
        print("TTL: %d, Source: " %ttl, packet[IP].src)
        ttl+= 1
```

PROBLEMS 10 OUTPUT DEBUG CONSOLE TERMINAL PORTS JUPYTER

```
TTL: 128, Source:  8.8.8.8
TTL: 129, Source:  8.8.8.8
^CTraceback (most recent call last):
  File "/home/seed/Lab2/Executables/traceroute.py", line 12, in <module>
    packet = sr1(ip / icmp, timeout=2, verbose=0)
             ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/scapy/sendrecv.py", line 663, in sr1
    ans, _ = sr(*args, **kargs)
             ^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3/dist-packages/scapy/sendrecv.py", line 650, in sr
    s = conf.L3socket(promisc=promisc, filter=filter,
        ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
```

```
  File "/usr/lib/python3/dist-packages/scapy/arch/linux.py", line 500, in __init__
    self.ins.bind((self.iface, type))
KeyboardInterrupt
^C
root@ubuntu-s-4vcpu-8gb-amd-nyc1-01:/home/seed/Lab2/Executables# sudo python3 traceroute.py
TTL 1: No response
TTL: 2, Source:  10.71.5.156
TTL: 3, Source:  138.197.248.76
TTL: 4, Source:  143.244.192.152
TTL 5: No response
TTL: 6, Source:  143.244.225.19
TTL: 7, Source:  146.190.180.27
TTL: 8, Source:  142.251.249.123
TTL: 9, Source:  142.250.224.247
TTL: 10, Source:  8.8.8.8
root@ubuntu-s-4vcpu-8gb-amd-nyc1-01:/home/seed/Lab2/Executables#
```

```
73749 2025-03-21 11:20:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=129 (rep
73750 2025-03-21 11:20:… 8.8.8.8          ICMP  134.209.118.177  58 Echo (ping) reply    id=0x0000, seq=0/0, ttl=117 (rec
80432 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=1 (no re
80836 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=1 (no re
81159 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=1 (no re
81473 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=2 (no re
81474 2025-03-21 11:21:… 10.71.5.156       ICMP  134.209.118.177  72 Time-to-live exceeded (Time to live exceeded in trans
81478 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=3 (no re
81479 2025-03-21 11:21:… 138.197.248.76    ICMP  134.209.118.177  72 Time-to-live exceeded (Time to live exceeded in trans
81483 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=4 (no re
81484 2025-03-21 11:21:… 143.244.192.152   ICMP  134.209.118.177  72 Time-to-live exceeded (Time to live exceeded in trans
81488 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=5 (no re
81925 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=5 (no re
82297 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=5 (no re
82684 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=6 (no re
82685 2025-03-21 11:21:… 143.244.225.19    ICMP  134.209.118.177  72 Time-to-live exceeded (Time to live exceeded in trans
82686 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=7 (no re
82687 2025-03-21 11:21:… 146.190.180.27    ICMP  134.209.118.177  112 Time-to-live exceeded (Time to live exceeded in trans
82702 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=8 (no re
82703 2025-03-21 11:21:… 142.251.249.123   ICMP  134.209.118.177  72 Time-to-live exceeded (Time to live exceeded in trans
82709 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=9 (no re
82715 2025-03-21 11:21:… 142.250.224.247   ICMP  134.209.118.177  112 Time-to-live exceeded (Time to live exceeded in trans
82721 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=10 (repl
82722 2025-03-21 11:21:… 8.8.8.8          ICMP  134.209.118.177  58 Echo (ping) reply    id=0x0000, seq=0/0, ttl=117 (rec
82729 2025-03-21 11:21:… 134.209.118.177  ICMP  8.8.8.8          44 Echo (ping) request  id=0x0000, seq=0/0, ttl=11 (repl
82730 2025-03-21 11:21:… 8.8.8.8          ICMP  134.209.118.177  58 Echo (ping) reply    id=0x0000, seq=0/0, ttl=117 (rec
83692 2025-03-21 11:22:… 134.209.118.177  ICMP  154.213.200.14   106 Destination unreachable (Port unreachable)
86423 2025-03-21 11:23:… 134.209.118.177  ICMP  165.154.163.10    79 Destination unreachable (Port unreachable)
89172 2025-03-21 11:24:… 134.209.118.177  ICMP  146.88.241.121    86 Destination unreachable (Port unreachable)
93390 2025-03-21 11:24:… 134.209.118.177  ICMP  109.236.61.55     73 Destination unreachable (Port unreachable)
```

And I got a bunch of "Host administratively prohibited" messages along the way.

I think they don't like me :D

```
99785 2025-03-21 11:26:… 138.2.229.54  ICMP  134.209.118.177  96 Destination unreachable (Host administratively prohibited)
1004… 2025-03-21 11:26:… 138.2.229.54  ICMP  134.209.118.177  96 Destination unreachable (Host administratively prohibited)
```

Q4 Sniffing and-then Spoofing

Sniffing and-then Spoofing. You need two machines on the same LAN: the VM and the user container.

You will find that when you ping from the terminal, 10.9.0.99 will have a destination unreachable response. That is the expected result. Your program does not need to work for this IP. (You do not need to force it to work by performing ARP spoofing.) You will, however, need to explain why your program does not work for IP 10.9.0.99 (while it’s supposed to work for 1.2.3.4 and 8.8.8.8).

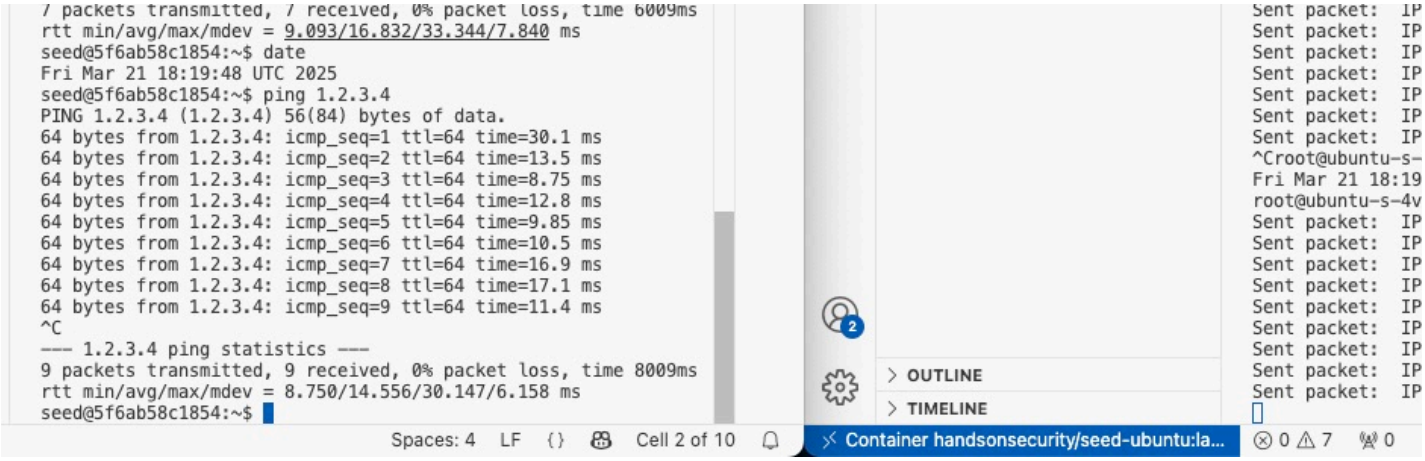
In this task, you will combine the sniffing and spoofing techniques to implement the following sniff-and-
then-spoof program. You need two machines on the same LAN. From machine A, you ping an IP X. This
will generate an ICMP echo request packet. If X is alive, the ping program will receive an echo reply, and
print out the response. Your sniff-and-then-spoof program runs on the attacker machine, which monitors
the LAN through packet sniffing. Whenever it sees an ICMP echo request, regardless of what the target IP
address is, your program should immediately send out an echo reply using the packet spoofing technique.
Therefore, regardless of whether machine X is alive or not, the ping program will always receive a reply,
indicating that X is alive. You need to write such a program in C, and include screenshots in your report to
show that your program works. Please also attach the code (with adequate amount of comments) in your
report.

4.1

```
#!/usr/bin/env python3
from scapy.all import *
def sniff_and_spoof(packet):
    if ICMP in packet:
        # Reverse source and destination
        ip = IP(src=packet[IP].dst, dst=packet[IP].src)

        # Create ICMP echo reply
        icmp = ICMP(type=0, id=packet[ICMP].id, seq=packet[ICMP].seq)

        if Raw in packet:
            raw_data = packet[Raw].load
        else:
            raw_data = ""

        new_packet= ip/icmp/raw_data

        send(new_packet, verbose=0)
        print("Sent packet: ", new_packet.summary())
pkt = sniff(filter="icmp and icmp[0] == 8", prn=sniff_and_spoof, iface="br-
407b98f0a521")
```

1- packet[IP].dst
2- packet[IP].src
3- type=0
4- packet[ICMP].id
5- packet[ICMP].seq
6- packet[Raw].load
7- ip/icmp/raw_data
8- icmp and icmp[0] == 8

4.2



4.3

Ping 10.9.0.99 and show screenshots of the output from your program and with the ping from the terminal. If this does not work, please explain why.

```
seed@5f6ab58c1854:~$ ping 10.9.0.99
PING 10.9.0.99 (10.9.0.99) 56(84) bytes of data.
From 10.9.0.5 icmp_seq=1 Destination Host Unreachable
From 10.9.0.5 icmp_seq=2 Destination Host Unreachable
From 10.9.0.5 icmp_seq=3 Destination Host Unreachable
From 10.9.0.5 icmp_seq=4 Destination Host Unreachable
ping: sendmsg: No route to host
From 10.9.0.5 icmp_seq=5 Destination Host Unreachable
From 10.9.0.5 icmp_seq=6 Destination Host Unreachable
^C
--- 10.9.0.99 ping statistics ---
9 packets transmitted, 0 received, +6 errors, 100% packet loss,
 time 8202ms
pipe 3
```

When our host pings an IP on the LAN, it wants to resolve the MAC from IP through ARP. Since no machine actually owns 10.9.0.99, ARP gets no reply.

Since ARP is never delivered, we see no ICMP requests from our attacker or wireshark, which is consistent since there is no poisoned arp cache.

When ip is outside LAN, the default gateway is the one tasked with responding to ARP requests, so icmp is delivered and we can spoof them.

4.4